



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/312,230	05/14/1999	MIKHAIL J. ATALLAH	P00619-US-0	2301

7590 05/07/2003

Thomas A. Walsh
ICE MILLER
One American Square
Box 82001
Indianapolis, IN 46282-0002

EXAMINER

SMITHERS, MATTHEWS

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 05/07/2003

10

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/312,230	ATALLAH ET AL. <i>SJ</i>
	Examiner	Art Unit
	Matthew B Smithers	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 14 May 1999.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-22,24-31 and 33 is/are rejected.
- 7) Claim(s) 23 and 32 is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 14 May 1999 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) The proposed drawing correction filed on _____ is: a) approved b) disapproved by the Examiner.
If approved, corrected drawings are required in reply to this Office action.
- 12) The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

- 14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
a) The translation of the foreign language provisional application has been received.
- 15) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s). _____.
2) <input checked="" type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449) Paper No(s) <u>2,89</u> .	6) <input type="checkbox"/> Other: _____.

DETAILED ACTION

Information Disclosure Statement

The information disclosure statement filed May 14, 199, January 15, 2002 and August 19, 2002 have been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-22, 24-31 and 33 are rejected under 35 U.S.C. 102(a) as being anticipated by "Speeding Up Secret Computations with Insecure Auxiliary Devices" by Matsumoto et al.

Regarding claim 1-2, 13-14, 18, 20, 24-25 and 28-29, Matsumoto shows a client (the second computer) disguises an argument "x" by applying an algorithm "I" to create "u" which is then sent to the server (the first computer). The server computes a result "v" using the disguised input "u" and sends the result "v" back to the client. The client then obtains the actual answer "y" by applying algorithm "F" to the result "v". (see page 499, Paragraph 3).

Regarding claim 3-12, 15-17, 19, 21-22, 26-27, 30-31 and 33, Matsumoto shows basic protocols where matrices are randomly generated at the client and matrix multiplication, linear equations or graph isomorphisms (where permutation matrix X satisfies $AX=XB$) are used in the process of obtaining the actual answer from an outsourced computation. (see page 499, Paragraph 3, page 500, Paragraph 4, 4.1(a), 4.1(b) and page 501, paragraph 4.1(c).)

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

Claims 1-2, 13-14, 18, 20, 24-25 and 28-29 are rejected under 35 U.S.C. 102(a) as being anticipated by “Fast Server-Aided Secret Computation Protocols for Modular Exponentiation” by Kawamura et al.

Regarding claims 1-2, 13-14, 18, 20, 24-25 and 28-29 Kawamura shows a system where a server performs computations for a client without knowing the client's secret information and the client computing the answer from the result computed by the server. (see page 499, Paragraph 3, page 500, Paragraph 4, 4.1(a), 4.1(b) and page 501, paragraph 4.1(c).)

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-2, 13-14, 18, 20, 24-25 and 28-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Netsolve: A Network for Solving Computational Science Problems" by Casanova et al and further in view of "On Hiding Information from an Oracle" by Abadi et al.

Regarding claims 1-2, 13-14, 18, 20, 24-25 and 28-29, Casanova teaches a client-server application designed to solve computational science problems over a network where the server supplies the computational resources needed to service the user's request (see Abstract, page 2, Introduction to page 6, Programming Interfaces and Figure 1). Casanove fails to specifically teach hiding the argument "x" from the server performing the outsourced computation. Abadi teaches a system where a server (the first computer/player B) computes a value for a client (second computer/player A) in such a way that player B cannot determine player A's input value, returns a result for the hiding value and the client further computes the actual answer from the serve computed result (see Abstract and page 4, paragraph 2. Basic definitions to page 6). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Abadi's hiding information from on oracle with Casanova's netsolve system in order to gain the gain the advantage of resources offered by a

computing center without having to reveal confidential data [see Abadi et al; page 2, Introduction, Suppose . . . data.]

Allowable Subject Matter

Claims 23 and 33 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter: The prior art fails to teach generating a cubic spline to provide at least one disguise function.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Abadi et al, "Secure circuit evaluation", discloses a protocol for securely communicating between two players.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone

numbers for the organization where this application or proceeding is assigned are (703) 746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Matthew B. Smithers
Matthew B Smithers
Primary Examiner
Art Unit 2134

May 2, 2003